IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA v. TAYLOR HUDDLESTON, Defendant.	Case No. 17-CR-34 Hon. Liam O'Grady Sentencing: February 23, 2018

POSITION OF THE UNITED STATES ON SENTENCING

Computer hacking is often seen as an individual crime committed by lone wolves with exceptional computer skills. In truth, hacking has increasingly become a group crime. Many hackers commit their crimes using malicious software (or "malware") that they did not and perhaps could not create themselves. And even those with the ability to develop malware often need assistance distributing it to the hackers who will ultimately use it to commit crimes. For over four years, the defendant, Taylor Huddleston, served both roles in the underground hacking community: he developed and distributed malware of his own, and he developed software that helped other malware developers distribute their products. Using the alias "AeonHack," Huddleston marketed both products on a website devoted to computer hacking called "Hackforums."

Huddleston's first product was a type of malware known as a remote access tool (or "RAT"). Huddleston's RAT allowed his hacker-clients to infect victim computers, steal sensitive information, and spy on the victims. In particular, the RAT enabled hackers to steal any information on their victims' computers, including passwords to online accounts, saved files, and all keystrokes typed into the infected computer. Huddleston's RAT even allowed his clients to surreptitiously activate the webcam on their victims' computer in order to literally see into their victims' homes. This frighteningly malicious product was used in over 100,000 computer intrusions and attempted computer intrusions.

Huddleston's second product, which he called "Net Seal," was a type of licensing software that was used to distribute malware. Licensing software enables software developers to control the distribution of their products so that only paying customers can have access. Net Seal was licensing software for malware developers: Huddleston advertised it exclusively on Hackforums and used it to distribute software that he knew to be malicious. For instance, Huddleston used Net Seal to help Zachary Shames distribute over 3,000 copies of his malicious keylogger. But Shames was just one of the malware developers whom Huddleston counted as a client. Huddleston used Net Seal to distribute over 2,500 software products, the overwhelming majority of which are believed to have been malicious.

The presentence report correctly calculated the defendant's total offense level as 27, resulting in a guidelines range of **70 to 87 months' imprisonment**. Because Mr. Huddleston spent years designing and selling products that harmed thousands of innocent people, the government respectfully submits that a sentence of **87 months' imprisonment** is necessary to reflect the seriousness of the offense and to protect the public from the growing threat of computer intrusions.

I. Offense of Conviction

A. Huddleston Designed and Sold Malware Called the NanoCore RAT

Beginning in 2013, Huddleston developed and distributed computer intrusion software known as the NanoCore Remote Access Tool (hereinafter, "NanoCore" or "Huddleston's RAT").

PSR ¶ 36. A remote access tool, or "RAT," is a program designed to allow a computer hacker to take complete control of a victim's computer just as if that hacker was sitting at the victim's keyboard. *Id.* RATs provide hackers with a backdoor into a victim's computer so that the hacker can spy on the victim, cause the victim's computer to run additional malicious software, or use the victim's computer to launch attacks on other computer systems. *Id.* Huddleston designed his RAT to include the following malicious features that he knew would be used to commit illegal computer crimes:

- A keylogger that allowed NanoCore users to record all keystrokes typed on their victims' computers;
- A password downloader that allowed NanoCore users to steal passwords that were saved on their victims' computers;
- A webcam feature that allowed NanoCore users to surreptitiously activate the webcam on their victims' computers in order to see into their victims' homes; and
- A file access feature that allowed NanoCore users to view, delete, download, and otherwise manipulate files stored on their victims' computers.

PSR ¶ 37.

In addition, Huddleston created a "plug-in" feature that enabled his clients to add their own functionalities to the NanoCore RAT and, unsurprisingly, his clients used that feature to add malicious functions. *Id.* ¶ 38. For instance, Huddleston was aware that NanoCore users had added a "ransomware feature" that enabled hackers using NanoCore to encrypt a victim's computer until the victim pays a ransom to the hacker. *Id.* Huddleston was also aware that NanoCore users added a "booter" or "stresser" feature that allowed NanoCore users to perpetrate distributed denial of service (DDoS) attacks using the computers they infected with NanoCore. *Id.* A DDoS attack occurs when malicious actors use networks of compromised computers that they control to overwhelm a target website or server with web traffic, thereby rendering the target website or server unavailable to legitimate users.

By developing NanoCore and distributing it to people whom he knew to be computer hackers, Huddleston knowingly and intentionally aided and abetted thousands of unlawful computer intrusions and attempted unlawful computer intrusions. PSR ¶ 40. For example, Huddleston's RAT was used in a massive spear phishing scheme[1] that targeted over 6,000 computers. *Id.* ¶ 41. As part of that scheme, a hacker sent an email to over 6,000 clients of a major oil and gas company purporting to be an email from the oil company and attaching an invoice. *Id.* ¶ 42. If the client clicked on the link containing the purported invoice, they would inadvertently install Huddleston's RAT onto their computers and enable the hacker to steal their passwords, record their key strokes, copy or delete their files, and even to watch them through their own computer's webcam. *Id.* This phishing scheme using Huddleston's RAT does not appear to have been an isolated incident. Palo Alto Networks, a major cybersecurity firm, reported that Huddleston's NanoCore RAT was used in a series of phishing emails sent during tax season that purported to contain tax-related documents. *See* Anthony Kasza and Tyler Halfpop, *NanoCoreRAT Behind an Increase in Tax-Themed Phishing Emails* (Feb. 9, 2016), available at, https://researchcenter.paloaltonetworks.com/2016/02/nanocorerat-behind-an-increase-in-tax-themed-phishing-e-mails/.

[1] A spear phishing scheme is a scheme to trick victims into downloading malicious software onto their computers or disclosing sensitive information by sending communications, typically emails, that purport to be from a friendly source. Spear phishing messages often ask the victim to click on a link or to open an attachment that looks benign but in fact contains a request to download malicious software.

Symantec, a major antivirus company that owns and administers the popular "Norton" antivirus software, informed the government that it detected Huddleston's NanoCore RAT on over 107,813 of its clients' computers. *See* Ex. 1 (Letter from Symantec to the FBI). This means that Huddleston's RAT was installed on 107,813 computers running Norton antivirus software but that the software detected and quarantined the RAT at some point. Because Symantec is not able to distinguish between instances when the RAT was detected before it was able to actually steal any information from the victim computer versus those in which the RAT was detected after information may have been stolen, the government is unable to state how many of these 107,000-plus attempted computer intrusions were successful. It is certainly possible that, in most cases, Huddleston's RAT was detected and quarantined before it could do any damage. Still, the fact that a single antivirus company detected Huddleston's RAT on over 107,000 of their clients' computers gives a sense of the extent to which Huddleston's RAT was used in hacking schemes.

B. Huddleston Created a Product Called "Net Seal" to Distribute Malware Developed by Others.

In addition to developing and distributing his own malware, Huddleston developed a type of licensing software, which he named "Net Seal," that helped other malware developers (Huddleston's clients) distribute their products. PSR ¶ 25. Licensing software enables software developers to control the distribution of their products so that only paying customers can have access. Huddleston set up his Net Seal licensing software to automatically send emails to the purchasers of his clients' software. PSR ¶ 31. Those emails contained a license serial code and instructions for how to download and activate the software. *Id.* The purpose of these emails was to help with the orderly, effective, and profitable distribution of the software developed by Huddleston's clients. *Id.*

The problem was that Huddleston's clients were malware developers, and, as Huddleston was well aware, the products they distributed using Net Seal were malicious. For instance, Huddleston used Net Seal to distribute Zachary Shames's malicious keylogger to over 3,000 people who in turn used it to infect and steal information from over 16,000 victim computers. *Id.* ¶ 32. In return, Shames made 1269 payments to Huddleston via PayPal. *Id.* ¶ 28. All the while Huddleston was well aware of the malicious nature of Shames's product. Shames openly touted the malicious nature of his product on Hackforums (a website that was central to Huddleston's business and which Huddleston frequented regularly), and the two formed a private group on the messaging service Skype where they and a select group of malware developers could discuss malware and hacking. PSR ¶¶ 29, 34(d).

Shames was not the only malware developer to distribute his product using Net Seal. Huddleston has admitted that he provided Net Seal to several other malware developers who used it to distribute malware that was repeatedly used to commit unlawful and unauthorized computer intrusions and to damage victim computers. *Id.* ¶ 33. Huddleston further admitted that, for the entire four-year period that he operated Net Seal, he "acted with the purpose of furthering and aiding and abetting these illegal and unauthorized computer intrusions." *Id.* Huddleston sought malware developer clients by advertising Net Seal on Hackforums, a forum where members can obtain hacking tools and chat about hacking. *Id.* ¶ 27. Unsurprisingly, this resulted in Huddleston developing a client list for Net Seal that was chock-full of malware developers. The following is a sample of the types of malicious products Huddleston distributed during the four years he owned Net Seal:

- **Keyloggers:** Keyloggers are malware designed to steal text typed into an infected computer. The stolen information frequently includes passwords to email and banking accounts. The "Limitless Logger" created by Zachary Shames is one example of a particular keylogger distributed by Huddleston. But there appears to have been many others: Huddleston's Net Seal client list contained **104 products** whose brand names included the word "keylogger," "logger," or "monitor."

- **Remote Access Tools (RATs):** RATs are malware that give hackers complete control of a victim's computer for the purpose of performing various malicious activities, including stealing passwords, stealing keystrokes, altering or deleting documents, searching for and stealing particular documents, or using the victim computer to launch attacks on other computers. Huddleston's own "NanoCore RAT" is an example of a RAT, but he appears to have distributed many others. The Net Seal client list contained **128 products** whose brand names included the word "RAT." One of these RATs was called "LuminosityLink." It was also advertised on Hackforums and is believed to have been used in at least 50,000 attempted computer intrusions. *See* Josh Grunzweig, *Investigating the LuminosityLink Remote Access Trojan* (July 8, 2016), available at https://researchcenter.paloaltonetworks.com/2016/07/unit42-investigating-the-luminositylink-remote-access-trojan-configuration/.

- **Crypters:** Crypters are software designed to disguise malware so that it cannot be recognized and blocked by antivirus software. Net Seal's client list contained **322 products** whose brand names included the word "crypter." Net Seal's client list also included a product called "Cyptex Reborn," which is a crypter developed by Goncalo Esteves of the United Kingdom. Mr. Esteves recently pled guilty to computer misuse offenses in Blackfriars Crown Court in London. *See* Tara Seals, *Man Running Product Testing Service for Malware Made Thousands*, Info Security, available at https://www.infosecurity-magazine.com/news/man-running-product-testing/.

- **Booters/Stressers:** "Booters" and "Stressors" are malware designed to allow hackers to take control of an infected computer and use it to conduct DDoS attacks[2] against other computers or websites. The Net Seal client list contained **133 products** whose brand names included the word "booter" or "stresser."

- **Ransomware:** Ransomware is malware that enables hackers to encrypt a victim's computer until the victim pays a ransom to the hacker. The Net Seal client list contained **two products** whose brand names included the word "ransom."

In addition, Net Seal's client list contained scores of products whose names contained other words that are highly indicative of malware, including "hack," "trojan," "stealer," "miner," "bot," "espionage," and "DDoS."

[2] As noted above, a DDOS attack is when malicious actors use networks of compromised computers that they control to overwhelm a target website or sever with traffic, with the goal of causing the target website or server to collapse.

II. Guidelines Range

Huddleston pled guilty in this Court to aiding and abetting computer intrusions, in violation of 18 U.S.C. § 1030(a)(5)(A). PSR ¶ 1. The maximum penalty for this offense is 10 years' imprisonment, a $250,000 fine, and 3 years' supervised release. PSR ¶ 87.

A. Calculation By Probation Officer

The probation officer correctly calculated the defendant's offense level as follows:

Guideline	**Offense Level**
Base Offense Level (U.S.S.G § 2B1.1(a)(1))	6
Loss amount above $1.5 and $3.5 million (U.S.S.G § 2B1.1(b)(1)(I))	+16
Offense involved 10 or more victims (U.S.S.G § 2B1.1(b)(2)(A))	+2
The defendant was convicted of an offense under 18 U.S.C. § 1030(a)(5)(A). (U.S.S.G § 2B1.1(b)(18)(A)(ii))	+4
The defendant used a special skill, in a manner that significantly facilitated the commission or concealment of the offense. (U.S.S.G § §3B1.3)	+2
Acceptance of responsibility (Section 3E1.1)	-3
TOTAL	**27**

PSR ¶¶ 51-63.

B. Enhancement for Loss Amount

The parties have stipulated, and the probation officer has agreed, that a sixteen-point enhancement is appropriate under U.S.S.G. § 2.B1.1(b)(1)(I) because the loss attributable to the defendant was between $1.5 and $3.5 million. In particular, probation determined that the provable loss attributable to the defendant is $3,369,400. PSR ¶ 53. This is based on the 16,847 computer intrusions committed with Zachary Shames's keylogger which Huddleston admitted to aiding and abetting. *Id.* ¶¶ 24-25, 32. In connection with Shames's sentencing, the government determined that the reasonable costs to repair a computer infected with a keylogger like Shames's was approximately $200.00. This figure is based on information the FBI received from four private computer service companies that offer malware remediation services. The estimate includes the cost of backing up personal files from the infected computer, wiping the computer's hard drive, and then reinstalling the computer's operating system. Consideration of such costs is appropriate under the guidelines, which counsel that loss amount for computer intrusions should include "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense." U.S.S.G. § 2B1.1, note 3(A)(v)(III); *accord* 18 U.S.C. § 1030(e)(11). Accordingly, the parties reached the loss figure of $3,369,400 by multiplying the number of computers infected Shames's Keylogger that Huddleston helped distribute (16,847) by the cost of repairing each of those computers ($200).

As noted above, Huddleston used Net Seal to distribute many other malicious products in addition to Shames's keylogger. Plus, Huddleston himself designed and distributed a RAT that appears to have been used in over 107,000 actual or attempted computer intrusions. However, pursuant to the plea agreement and in order to avoid unnecessary and time-consuming litigation, the government and defense counsel have agreed to a provable loss figure of $3,369,400 and the accompanying 16-point enhancement.

C. Enhancement for Use of a Special Skill

The probation officer appropriately recommends a two-point enhancement because Huddleston "used a special skill … in a manner that significantly facilitated the commission or concealment of the offense." U.S.S.G. § 3B1.3. Courts have repeatedly held that a special skill enhancement is appropriate where, as here, the defendant has knowledge of computers that far exceeds that of the general public and uses that knowledge to commit the crime. *See United States v. O'Brien*, 435 F.3d 36, 42 (1st Cir. 2006) (upholding special skill enhancement for defendant who worked as a computer consultant was thus "plausibly found to have had such skills beyond those possessed by an ordinary computer user"); *United States v. Petersen*, 98 F.3d 502, 506 (9th Cir. 1996) (upholding special skill enhancement for defendant who had no "formal training in computers" and who did not have the ability to "create [computer] programs," but who "obviously has an extraordinary knowledge of how computers work").

Following these precedents, this Court appropriately applied the special skill enhancement to Zachary Shames. *See United States v. Shames*, 16-cr-289 (E.D.Va. 2018). Like Zachary Shames and the defendants in *O'Brien* and *Petersen*, Huddleston clearly has "substantial knowledge in software development," PSR ¶ 48, as found by probation. Huddleston's skills in computer programing are evident from the fact that he was able to code two software programs that were highly popular among cybercriminals. The NanoCore RAT had hundreds of users and Net Seal had thousands. The very fact that thousands of computer-savvy hackers and malware developers were willing to pay Huddleston to use his software products shows that Huddleston possesses computer skills that are "not possessed by members of the general public." U.S.S.G. § 3B1.3 note 4. Moreover, as the Court appropriately found in the context of Shames's sentencing, one can have specialized skills in computer hacking without any formal training or licenses. *See also Petersen*, 98 F.3d at 507 ("substantial education, training or licensing … is not an absolute prerequisite for a special skill adjustment. Despite Petersen's lack of formal training or licensing, his sophisticated computer skills can reasonably be equated to the skills possessed by pilots, lawyers, chemists, and demolition experts for purposes of § 3B1.3"); *United States v. Malgoza*, 2 F.3d 1107, 1111 (11th Cir.1993) (defendant's advanced level of radio operating ability constitutes a special skill).

III. Sentencing Recommendation

As the Court is well aware, the Sentencing Guidelines are advisory, and just one factor that must be considered along with the other factors set forth in 18 U.S.C. § 3553(a).[3] Of these factors, the nature of the offense and the need to deter other malware developers are particularly relevant.

A. The Sentence Should Reflect Huddleston's Role in Invading the Privacy and Endangering the Data Security of Thousands of Victims.

It is difficult to calculate the full harm caused by Huddleston's malicious products. Huddleston's RAT, Shames's Keylogger, and the various other malicious products that Huddleston distributed via Net Seal, were all designed to steal sensitive information from victims' computers, such as the content of any message the victim typed while his/her computer was infected, and the victim's banking, email, and social media passwords. Online banking passwords can and often are used to empty a victim's bank account. And email and social media passwords are frequently used to spy on, to harass, and to blackmail victims. Access to a victim's email personal account, for instance, might provide a malicious actor with embarrassing information about the victim and would almost certainly provide the

[3] The § 3553(a) factors include: the nature and circumstances of the offense and the history and characteristics of the defendant; the need for the sentence imposed to reflect the seriousness of the offense, to promote respect for the law, to provide just punishment for the offense, to afford adequate deterrence to criminal conduct, to protect the public from further crimes of the defendant, and to provide the defendant with needed training, medical care, or other treatment; the kinds of sentences available; the kinds of sentence and the sentencing range established for the type of offense committed; any pertinent policy statement; the need to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct; and the need to provide restitution to any victims of the offense.

malicious actor with the victim's home address. The defense will no doubt characterize these dangers as speculative, but stealing passwords was a central purpose of Huddleston's RAT, Shames's keylogger, and several other products Huddleston distributed. Huddleston unleashed these malicious tools onto the public for his own profit despite knowing the clear dangers they posed to innocent people.

Huddleston's own RAT included additional features that were especially frightening: it enabled Huddleston's clients to steal files saved on the victims' computers, including the victims' pictures and videos, and even to activate the webcams on the victims' computers without displaying the webcam's light or any other sign that the camera was on. PSR ¶ 37(c). It is not difficult to imagine the egregious invasions of privacy made possible by this technology. In fact, in 2014, an individual named Marlen Rappa was convicted of using a RAT similar to Huddleston's RAT to activate the web cameras of several victims and capture images of them engaging in sexual activity in their bedrooms. *See United States v. Rappa*, 14-CR-544 (VC) (S.D.N.Y), Dkt. No 30 (Government's Sentencing Memorandum), at 3. Rappa also used the RAT to steal nude and/or sexually explicit photographs that the victims—primarily young women—had saved on their computers. *Id.* This sort of spying was, at minimum, a foreseeable use of the webcam and file-stealing features that Huddleston included in his RAT and, at worst, their intended purpose.

Malware developers like Huddleston are the root cause of computer hacking. Many hackers do not have the technical ability to create the malware they use to hack computers; just as the overwhelming majority of people who use any other type of software do not have the ability to build the software themselves. By creating his own malware and helping others distribute theirs, Huddleston exponentially increased the number of actors with the ability to engage in computer hacking. Huddleston's sentence should reflect the harm that he helped others inflict on innocent people.

B. The Sentence Should Be Sufficient to Deter Other Malware Developers.

In the cybercrime world, malware developers are at the heart of the problem. They provide the technical expertise that others use to victimize the public. Like the defendant, they often sell their products online using a pseudonym (the defendant used the name "AeonHack"), and are thus able to make a lot of money from the comfort and anonymity of their living rooms (the defendant admitted to receiving at least $88,739.59 in criminal proceeds). Like the defendant, these criminals often operate with impunity for years and begin to feel invincible. Unfortunately, high rewards and relatively low risk of detection are basic features of cybercrime that are not going to change anytime soon. The only way to affect the cost-benefit analysis of these crimes is to impose meaningful sentences on those who are caught. If the Court does so, there is every reason to believe that many would-be criminals will get the message. Computer hackers are among the most sophisticated criminals in the world and are known to closely monitor the government's response to cybercrime and plan accordingly. Achieving general deterrence in this area therefore appears particularly promising. *See United States v. Martin*, 455 F.3d 1227, 1240 (11th Cir. 2006) (Because "economic and fraud-based crime are more rational, cool, and calculated than sudden crimes of passion or opportunity, these crimes are prime candidates for general deterrence").

IV. Conclusion

For the forgoing reasons, the government respectfully recommends a sentence of **87 months' imprisonment**, which is the high-end guidelines range of 70 to 87 months' imprisonment, as well as an agreed-upon forfeiture order of $88,739.59.

Tracy Doherty-McCormick
Acting United States Attorney

By: /s/
Kellen S. Dwyer
Assistant United States Attorney
United States Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, Virginia 22314
(703) 299-3700
kellen.dwyer@usdoj.gov

Catherine Alden Pelker, Trial Attorney
U.S. Department of Justice, Criminal Division
Computer Crime & Intellectual Property Section

February 14, 2018

Certificate of Service

I hereby certify that on February 14, 2018, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of filing (NEF) to counsel of record for the defense.

I also certify that on February 16, 2018, I will send a true and correct copy of the foregoing by e-mail to the following:

Jennifer Lyerly
United States Probation Officer
Jennifer_Lyerly@vaep.uscourts.gov

By: ______/s/_________________
Kellen S. Dwyer
Assistant United States Attorney
United States Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, Virginia 22314
(703) 299-3700
kellen.dwyer@usdoj.gov